I CLAIM:

1. A method for enhancing trust in communications between a client device and a trusted server, comprising:

(a) generating a one-time password for use in communication from the device to the server;

(b) generating at least one one-time request-authentication datum comprising a function of at least a portion of a previous response from the server to a previous request from the device; and

(c) generating at least one one-time response-authentication datum comprising a function of at least a portion of at least one one-time password.

2. The method of claim 1, wherein said one-time request-authentication datum comprises a function of an encryption key.

3. The method of claim 1, wherein said one-time response-authentication datum comprises a function of an encryption key.

4. A method for enhancing trust in communicating a data request from a client device, comprising:

(a) generating a one-time password; and

(b) generating at least one one-time request-authentication datum comprising a function of at least a portion of a previous response from a trusted server to a previous request from the device.

5. The method of claim 4, wherein said one-time request-authentication datum comprises a function of an encryption key.

6. A method for enhancing trust in communicating a response from a request from a client device to a trusted server, comprising:

(a) receiving a request comprising a function of at least a portion of at least one one-time password shared between the device and said server; and

(b) generating at least one one-time response-authentication datum comprising a function of at least a portion of at least one one-time password.

7. The method of claim 6, wherein said one-time response-authentication datum comprises a function of an encryption key.

8. The method of claim 6, wherein said request comprises an encrypted secret datum, wherein said server decrypts said encrypted secret datum to recover said secret datum.

9. The method of claim 8, wherein a subsequent request comprises a function of at least a portion of at least one one-time password comprising at least a portion of at least one secret datum.

10. The method of claim 6, wherein the one-time password comprised within the request is used by the server to locate an entry in its database corresponding to the particular client device.

11. A method for resynchronizing communication between a client device and a trusted server, comprising:

(a) supplying a one-time password for use in communication from the device to the server;

(b) supplying at least one one-time request-authentication datum comprising a function of at least a portion of a previous response from the server to a previous request from the device; and

(c) supplying at least one one-time response-authentication datum comprising a function of at least a portion of at least one one-time password.

12. A method for enhancing trust in transmission of a resynchronization request from a client device, comprising:

(a) supplying a one-time password; and

(b) supplying at least one one-time request authentication datum comprising a function of at least a portion of a previous response from a trusted server to a request from the device.

13. The method of claim 12, wherein said resynchronization request comprises an encrypted resynchronization datum that replaces a previous resynchronization datum.

14. A method for enhancing trust in transmission of a resynchronization response from a trusted server, comprising:

(a) receiving a request comprising a one-time password associated with a client device; and

(b) supplying at least one one-time response-authentication datum comprising a function of at least a portion of at least one one-time password.

15. The method of claim 14, wherein said resynchronization response comprises an encrypted resynchronization datum that replaces a previous resynchronization datum.

16. A system for enhancing trust in communications between a client device and a trusted server, comprising:

(a) means for establishing a network connection between the client device and the server; and

(b) means for conducting communications of data with the client device over the network connection,

wherein said communications between the device and the server are conducted in accordance with a method comprising:

(i) generating a one-time password for use in communication from the device to the server;

(ii) generating at least one one-time request-authentication datum comprising a function of at least a portion of a previous response from the server to a previous request from the device; and

(iii) generating at least one one-time response-authentication datum comprising a function of at least a portion of at least one one-time password.

17. The system of claim 16, further comprising

(a) an encryption algorithm, and

(b) means for downloading said encryption algorithm to the client computer over said network connection,

wherein said means for conducting communications of data with the client computer over the network connection is in accordance with said encryption algorithm and wherein said communications between the device and the server are conducted on an encrypted basis.

18. The system of claim 16, wherein said one-time request-authentication datum comprises a function of an encryption key.

19. The system of claim 16, wherein said one-time response-authentication datum comprises a function of an encryption key.

20. A system for enhancing trust in communicating a data request from a client device, comprising:

(a) means for establishing a network connection between the client device and a trusted server; and

(b) means for conducting communications of data with the client device over the network connection,

wherein said communications between the device and the server are conducted in accordance with a method comprising:

(i) generating a one-time password; and

(ii) generating at least one one-time request-authentication datum comprising a function of at least a portion of a previous response from a trusted server to a previous request from the device.

21. The system of claim 20, further comprising

(a) an encryption algorithm, and

(b) means for downloading said encryption algorithm to the client computer over said network connection,

wherein said means for conducting communications of data with the client computer over the network connection is in accordance with said encryption algorithm and wherein said communications between the device and the server are conducted on an encrypted basis.

22. The system of claim 20, wherein said one-time request-authentication datum comprises a function of an encryption key.

23. A system for enhancing trust in communicating a response from a request from a client device to a trusted server, comprising:

(a) means for establishing a network connection between the client device and the server; and

(b) means for conducting communications of data with the client device over the network connection,

wherein said communications between the device and the server are conducted in accordance with a method comprising:

(i) receiving a request comprising a function of at least a portion of at least one one-time password shared between the device and said server; and

(ii) generating at least one one-time response-authentication datum comprising a function of at least a portion of at least one one-time password.

24. The system of claim 23, further comprising

(a) an encryption algorithm, and

(b) means for downloading said encryption algorithm to the client computer over said network connection,

wherein said means for conducting communications of data with the client computer over the network connection is in accordance with said encryption algorithm and wherein said communications between the device and the server are conducted on an encrypted basis.

25. The system of claim 23, wherein said one-time response-authentication datum comprises a function of an encryption key.

26. The system of claim 23, wherein said request comprises an encrypted secret datum, wherein said server decrypts said encrypted secret datum to recover said secret datum.

27. The system of claim 26, wherein a subsequent request comprises a function of at least a portion of at least one one-time password comprising at least a portion of at least one secret datum.

28. The method of claim 23, wherein the one-time password comprised within the request is used by the server to locate an entry in its database corresponding to the particular client device.

29. A system for resynchronizing communication between a client device and a trusted server, comprising:

(a) means for establishing a network connection between the client device and the server; and

(b) means for conducting communications of data with the client device over the network connection,

wherein said communications between the device and the server are conducted in accordance with a method comprising:

(i) supplying a one-time password for use in communication from the device to the server;

(ii) supplying at least one one-time request-authentication datum comprising a function of at least a portion of a previous response from the server to a previous request from the device; and

(iii) supplying at least one one-time response-authentication datum comprising a function of at least a portion of at least one one-time password.

30. The system of claim 29, further comprising

(a) an encryption algorithm, and

(b) means for downloading said encryption algorithm to the client computer over said network connection,

wherein said means for conducting communications of data with the client computer over the network connection is in accordance with said encryption algorithm and wherein said communications between the device and the server are conducted on an encrypted basis.

31. A system for enhancing trust in transmission of a resynchronization request from a client device, comprising:

(a) means for establishing a network connection between the client device and a trusted server; and

(b) means for conducting communications of data with the client device over the network connection,

wherein said communications between the device and the server are conducted in accordance with a method comprising:

(i) supplying a one-time password; and

(ii) supplying at least one one-time request authentication datum comprising a function of at least a portion of a previous response from the server to a request from the device.

32. The system of claim 31, further comprising

(a) an encryption algorithm, and

(b) means for downloading said encryption algorithm to the client computer over said network connection,

wherein said means for conducting communications of data with the client computer over the network connection is in accordance with said encryption algorithm and wherein said communications between the device and the server are conducted on an encrypted basis.

33. The system of claim 31, wherein said resynchronization request comprises an encrypted resynchronization datum that replaces a previous resynchronization datum.

34. A system for enhancing trust in transmission of a resynchronization response from a trusted server, comprising:

(a) means for establishing a network connection between a client device and the server; and

(b) means for conducting communications of data with the client device over the network connection,

wherein said communications between the device and the server are conducted in accordance with a method comprising:

(i) receiving a request comprising a one-time password associated with a client device; and

(ii) supplying at least one one-time response-authentication datum comprising a function of at least a portion of at least one one-time password.

35. The system of claim 34, further comprising

(a) an encryption algorithm, and

(b) means for downloading said encryption algorithm to the client computer over said network connection,

wherein said means for conducting communications of data with the client computer over the network connection is in accordance with said encryption algorithm and wherein said communications between the device and the server are conducted on an encrypted basis.

36. The system of claim 34, wherein said resynchronization response comprises an encrypted resynchronization datum that replaces a previous resynchronization datum.